

CLAIMS

- Sub  
a2
1. A method of obtaining proof of group membership in a computer system, comprising the steps of:
    - A. presenting by a requester to an on-line server associated with a group a request for a certificate certifying that a particular entity is a member of the group;
    - B. determining by the server whether the entity is a member of the group; and
    - C. issuing by the server a group membership certificate to the requester if the server determines that the entity is a member of the group.
  2. A method of obtaining proof of group non-membership in a computer system, comprising the steps of:
    - A. presenting by a requester to an on-line server associated with a group a request for a certificate certifying that a particular entity is not a member of the group;
    - B. determining by the server whether the entity is not a member of the group; and
    - C. issuing by the server a group non-membership certificate to the requester if the server determines that the entity is not a member of the group.
  3. A method for determining entity membership in a group, wherein a server associated with the group performs the step of making a dynamic decision on membership in the group of a particular entity.
  4. The method of claim 3, wherein the dynamic decision-making step includes obtaining by the server proof of entity membership in a second group.
  5. The method of claim 4, wherein the proof of entity membership comprises a group membership certificate.

1 6. The method of claim 4, wherein the proof of entity membership comprises a  
2 group membership list.

1 7. The method of claim 3, wherein the dynamic decision-making step includes ob-  
2 taining by the server proof of entity non-membership in a second group.

1 8. The method of claim 7, wherein the proof of entity non-membership comprises a  
2 group non-membership certificate.

1 9. The method of claim 7, wherein the proof of entity non-membership comprises a  
2 group membership list.

1 10. The method of claim 3, wherein the server performs the step of making a dynamic  
2 decision upon a request from a requester, and wherein the requester performs the step of  
3 presenting to the server proof of entity membership in a second group.

1 11. The method of claim 10, wherein the proof of entity membership comprises a  
2 group membership certificate.

1 12. The method of claim 10, wherein the proof of entity membership comprises a  
2 group membership list.

1 13. The method of claim 3, wherein the server performs the step of making a dynamic  
2 decision upon a request from a requester, and wherein the requester performs the step of  
3 presenting to the server proof of entity non-membership in a second group.

1 14. The method of claim 13, wherein the proof of entity non-membership comprises a  
2 group non-membership certificate.

1 15. The method of claim 13, wherein the proof of entity non-membership comprises a  
2 group membership list.

1 16. A computer system wherein a group membership certificate is issued by an on-  
2 line certification authority upon request.

1 17. A computer system wherein a group non-membership certificate is issued by an  
2 on-line certification authority upon request.

1 18. A computer system wherein a server associated with a group makes a dynamic  
2 decision on membership in the group of a particular entity.

1 19. The system of claim 18 wherein the server obtains proof of entity membership in  
2 a second group.

1 20. The system of claim 19 wherein the proof of entity membership is a group mem-  
2 bership certificate.

1 21. The system of claim 19 wherein the proof of entity membership is a group mem-  
2 bership list.

1 22. The system of claim 18 wherein the server obtains proof of entity non-  
2 membership in a second group.

1 23. The system of claim 22 wherein the proof of entity non-membership is a group  
2 non-membership certificate.

1 24. The system of claim 22 wherein the proof of entity non-membership is a group  
2 membership list.

1 25. The system of claim 18 wherein the server makes the dynamic decision on a re-  
2 quest from a requester, and wherein the requester presents to the server proof of entity  
3 membership in a second group.

1 26. The system of claim 25 wherein the proof of entity membership is a group mem-  
2 bership certificate.

1 27. The system of claim 25 wherein the proof of entity membership is a group mem-  
2 bership list.

1 28. The system of claim 18 wherein the server makes the dynamic decision on a re-  
2 quest from a requester, and wherein the requester presents to the server proof of entity  
3 non-membership in a second group.

1 29. The system of claim 28 wherein the proof of entity non-membership is a group  
2 non-membership certificate.

1 30. The system of claim 28 wherein the proof of entity non-membership is a group  
2 membership list.

1 31. A method of operating an on-line server on a computer network, said server asso-  
2 ciated with a group and performing the steps of:

3 A. receiving a request from a network device for proof of membership of a client  
4 in the group;

5 B. making a dynamic decision on whether the client is a member of the group;  
6 and

7 C. issuing to the network device, if the server decides that the client is a member  
8 of the group, a group membership certificate proving that the client is a mem-  
9 ber of the group.

1 32. The method of claim 31 wherein the network device is the client, said client sub-  
2 sequently presenting to a resource server a request for access to a resource on the resource  
3 server, said request including the group membership certificate.

1 33. The method of claim 31 wherein the network device is a resource server receiving  
2 a request from a client seeking access to a resource on the resource server, said resource  
3 server validating the group membership certificate and authorizing client access to the  
4 resource.

1 34. A method of operating an on-line server on a computer network, said server asso-  
2 ciated with a group and performing the steps of:

3 A. receiving a request from a network device for proof of membership of a client  
4 in the group;

5 B. making a dynamic decision on whether the client is a member of the group;  
6 and

7 C. issuing to the network device, if the server decides that the client is a member  
8 of the group, a group membership list proving that the client is a member of  
9 the group.

1 35. The method of claim 34 wherein the network device is the client, said client sub-  
2 sequently presenting to a resource server a request for access to a resource on the resource  
3 server, said request including the group membership list.

1 36. The method of claim 34 wherein the network device is a resource server receiving  
2 a request from a client seeking access to a resource on the resource server, said resource  
3 server validating the group membership list and authorizing client access to the resource.

1 <sup>37</sup>  
~~38.~~ A method of operating an on-line server on a computer network, said server asso-  
2 ciated with a group and performing the steps of:

- 3 A. receiving a request from a network device for proof of non-membership of a  
4 client in the group;  
5 B. making a dynamic decision on whether the client is not a member of the  
6 group; and  
7 C. issuing to the network device, if the server decides that the client is not a  
8 member of the group, a group non-membership certificate proving that the cli-  
9 ent is not a member of the group.

1 <sup>38</sup>  
~~39.~~ The method of claim ~~38~~ <sup>37</sup> wherein the network device is the client, said client sub-  
2 sequently presenting to a resource server a request for access to a resource on the resource  
3 server, said request including the group non-membership certificate.

1 <sup>39</sup>  
~~40.~~ The method of claim ~~38~~ <sup>37</sup> wherein the network device is a resource server receiving  
2 a request from a client seeking access to a resource on the resource server, said resource  
3 server validating the group non-membership certificate and authorizing client access to  
4 the resource.

1 <sup>40</sup>  
~~41.~~ A method of operating an on-line server on a computer network, said server asso-  
2 ciated with a group and performing the steps of:  
3 A. receiving a request from a network device for proof of non-membership of a  
4 client in the group;  
5 B. making a dynamic decision on whether the client is not a member of the  
6 group; and

C. issuing to the network device, if the server decides that the client is not a member of the group, a group membership list proving that the client is not a member of the group.

41

40

42

The method of claim 41 wherein the network device is the client, said client subsequently presenting to a resource server a request for access to a resource on the resource server, said request including the group membership list.

42

40

43

The method of claim 41 wherein the network device is a resource server receiving a request from a client seeking access to a resource on the resource server, said resource server validating the group membership list and authorizing client access to the resource.

43

44

An on-line server on a computer network, said server associated with a group and comprised of:

A. means for receiving a request from a network device for proof of membership of a client in the group;

B. means for making a dynamic decision on whether the client is a member of the group; and

C. means for issuing to the network device, if the server decides that the client is a member of the group, a group membership certificate proving that the client is a member of the group.

44

43

45

The on-line server of claim 44 wherein the network device is the client, said client subsequently presenting to a resource server a request for access to a resource on the resource server, said request including the group membership certificate.

45

43

46

The on-line server of claim 44 wherein the network device is a resource server receiving a request from a client seeking access to a resource on the resource server, said

resource server validating the group membership certificate and authorizing client access to the resource.

46

47. An on-line server on a computer network, said server associated with a group and comprised of:

A. means for receiving a request from a network device for proof of membership of a client in the group;

B. means for making a dynamic decision on whether the client is a member of the group; and

C. means for issuing to the network device, if the server decides that the client is a member of the group, a group membership list proving that the client is a member of the group.

47

48. The on-line server of claim 47 wherein the network device is the client, said client subsequently presenting to a resource server a request for access to a resource on the resource server, said request including the group membership list.

46

48

49. The on-line server of claim 47 wherein the network device is a resource server receiving a request from a client seeking access to a resource on the resource server, said resource server validating the group membership list and authorizing client access to the resource.

46

49

50. An on-line server on a computer network, said server associated with a group and comprised of:

A. means for receiving a request from a network device for proof of non-membership of a client in the group;

B. means for making a dynamic decision on whether the client is not a member of the group; and



7 C. means for issuing to the network device, if the server decides that the client is  
8 not a member of the group, a group non-membership certificate proving that  
9 the client is not a member of the group.

50

1 ~~51.~~ The on-line server of claim ~~50~~<sup>49</sup> wherein the network device is the client, said client  
2 subsequently presenting to a resource server a request for access to a resource on the re-  
3 source server, said request including the group non-membership certificate.

51

1 ~~52.~~ The on-line server of claim ~~50~~<sup>49</sup> wherein the network device is a resource server  
2 receiving a request from a client seeking access to a resource on the resource server, said  
3 resource server validating the group non-membership certificate and authorizing client  
4 access to the resource.

52

1 ~~53.~~ An on-line server on a computer network, said server associated with a group and  
2 comprised of:

3 A. means for receiving a request from a network device for proof of non-  
4 membership of a client in the group;

5 B. means for making a dynamic decision on whether the client is not a member  
6 of the group; and

7 C. means for issuing to the network device, if the server decides that the client is  
8 not a member of the group, a group membership list proving that the client is  
9 not a member of the group.

53

1 ~~54.~~ The on-line server of claim ~~53~~<sup>52</sup> wherein the network device is the client, said client  
2 subsequently presenting to a resource server a request for access to a resource on the re-  
3 source server, said request including the group membership list.

54

1 ~~55.~~ The on-line server of claim ~~53~~<sup>58</sup> wherein the network device is a resource server  
2 receiving a request from a client seeking access to a resource on the resource server, said

resource server validating the group membership list and authorizing client access to the resource.

55

56. A computer data signal embodied in a carrier wave and representing a sequence of instructions that, when executed by a processor in a network device associated with a group, configures the network device to operate as an on-line server that:

- A. receives a request from a second network device for proof of membership of a client in the group;
- B. makes a dynamic decision on whether the client is a member of the group; and
- C. issues to the second network device, if the on-line server decides that the client is a member of the group, a group membership certificate proving that the client is a member of the group.

56

57. The computer data signal of claim 56 wherein the second network device is the client, said client subsequently presenting to a resource server a request for access to a resource on the resource server, said request including the group membership certificate.

55

57

58. The computer data signal of claim 56 wherein the second network device is a resource server, said resource server receiving a request from a client seeking access to a resource on the resource server, validating the group membership certificate, and authorizing client access to the resource.

53

58

59. A computer data signal embodied in a carrier wave and representing a sequence of instructions that, when executed by a processor in a network device associated with a group, configures the network device to operate as an on-line server that:

- A. receives a request from a second network device for proof of membership of a client in the group;
- B. makes a dynamic decision on whether the client is a member of the group; and

7 C. issues to the second network device, if the on-line server decides that the cli-  
8 ent is a member of the group, a group membership list proving that the client  
9 is a member of the group.

59

58

1 60. The computer data signal of claim 59 wherein the second network device is the  
2 client, said client subsequently presenting to a resource server a request for access to a  
3 resource on the resource server, said request including the group membership list.

60

58

1 61. The computer data signal of claim 59 wherein the second network device is a re-  
2 source server, said resource server receiving a request from a client seeking access to a  
3 resource on the resource server, validating the group membership list, and authorizing  
4 client access to the resource.

61

1 62. A computer data signal embodied in a carrier wave and representing a sequence of  
2 instructions that, when executed by a processor in a network device associated with a  
3 group, configures the network device to operate as an on-line server that:

4 A. receives a request from a second network device for proof of non-membership  
5 of a client in the group;

6 B. makes a dynamic decision on whether the client is not a member of the group;  
7 and

8 C. issues to the second network device, if the on-line server decides that the cli-  
9 ent is not a member of the group, a group non-membership certificate proving  
10 that the client is not a member of the group.

62

61

1 63. The computer data signal of claim 62 wherein the second network device is the  
2 client, said client subsequently presenting to a resource server a request for access to a  
3 resource on the resource server, said request including the group non-membership certifi-  
4 cate.

63

1 64. The computer data signal of claim 62 wherein the second network device is a re-  
2 source server, said resource server receiving a request from a client seeking access to a  
3 resource on the resource server, validating the group non-membership certificate, and  
4 authorizing client access to the resource.

61

64

1 65. A computer data signal embodied in a carrier wave and representing a sequence of  
2 instructions that, when executed by a processor in a network device associated with a  
3 group, configures the network device to operate as an on-line server that:

- 4 A. receives a request from a second network device for proof of non-membership  
5 of a client in the group;  
6 B. makes a dynamic decision on whether the client is not a member of the group;  
7 and  
8 C. issues to the second network device, if the on-line server decides that the cli-  
9 ent is not a member of the group, a group membership list proving that the cli-  
10 ent is not a member of the group.

65

1 66. The computer data signal of claim 65 wherein the second network device is the  
2 client, said client subsequently presenting to a resource server a request for access to a  
3 resource on the resource server, said request including the group membership list.

64

66

1 67. The computer data signal of claim 65 wherein the second network device is a re-  
2 source server, said resource server receiving a request from a client seeking access to a  
3 resource on the resource server, validating the group membership list, and authorizing  
4 client access to the resource.

64

ADD